gemalto
security to be free

# Data Breaches & Customer Loyalty 2018

## Social media companies believed to pose greatest risk for exposing data

# Social media companies believed to be vulnerable, with 61% of consumers saying they pose greatest risk for exposing data

A majority of consumers are willing to walk away from businesses entirely if they suffer a data breach, with retailers most at risk. Two-thirds (66%) are unlikely to shop or do business with an organization that experiences a breach where their financial and sensitive information is stolen. Retailers (62%), banks (59%), and social media sites (58%) are the most at risk of suffering consequences with consumers prepared to use their feet.

Consumers across all ages, 93% are placing the blame squarely on businesses and would think about acting against them. Social media sites worry consumers most, with 61% concerned companies in this space don't adequately protect consumer data, followed by banking websites (40%).

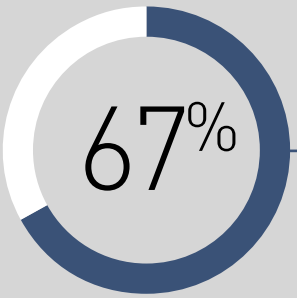
## Companies held responsible as consumers act

With the rising awareness of data protection and data privacy issues, consumers now believe the majority (70%) of responsibility for protecting their data rests on the company holding it. This has made data protection a major consideration for consumers when interacting with a brand, with 82% wanting organizations to have greater online security measures. These concerns are prompted by 91% believing that there are applications and websites they currently use which pose a risk to the protection and security of their personal identifiable information (PII).

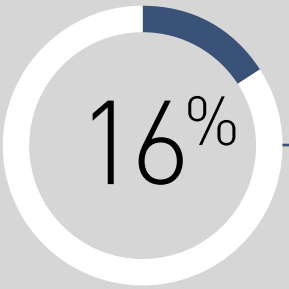
Despite consumers placing the responsibility firmly in the hands of organizations, only a quarter feel as though companies take the protection and security of customer data very seriously. Taking matters into their own hands, consumers are not giving businesses anywhere to hide, as the majority of respondents have either already provided organizations with feedback on what security methods they are offering (35%), have considered it (19%) or might in the future (33%).

Businesses have no choice but to improve their security if they want to address frustrated consumers that don't believe the onus is on them to change their security habits. Social media sites in particular have a battle on their hands to restore faith in their security and show consumers they're listening – failing to do so will spell disaster for the most flagrant offenders, as consumers take their business elsewhere.

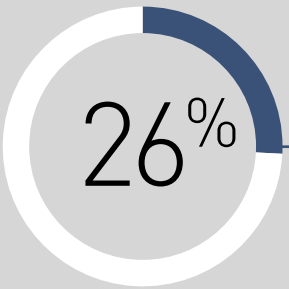
# Key Findings



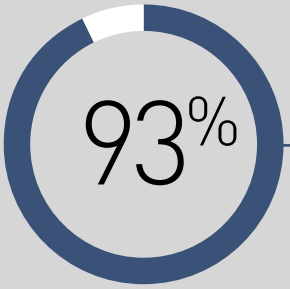

of 18-24 years olds would take legal action if personal details were stolen



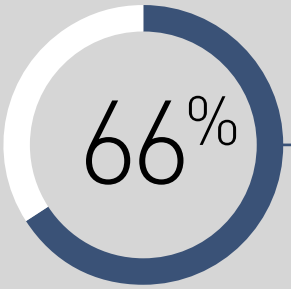

have been a victim of identity theft



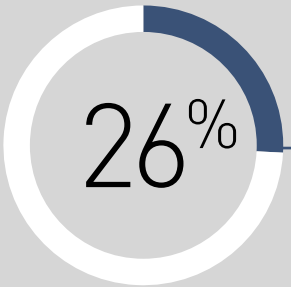

feel companies take the protection and security of customer data very seriously



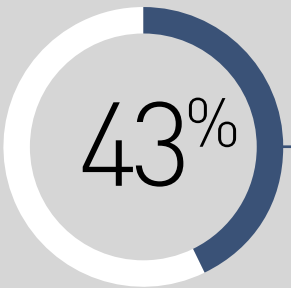

across all ages, would think about taking legal action



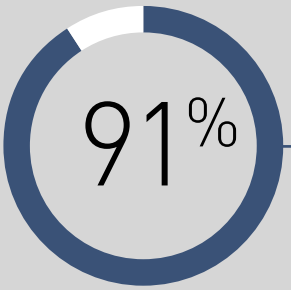

are unlikely to shop/ do business with an organization that experienced a breach where financial and sensitive information was stolen




have been a victim of fraudulent use of their financial information




of consumers who have been victim of a breach perceive this to have been from visiting a fraudulent website




of surveyed consumers believe that apps/websites pose a risk to their personal information

# Consumers and organizations' security measures to prevent breaches

## Use of online accounts

Most surveyed consumers actively use online accounts, including online/mobile banking (85%), social media accounts (82%) and/or online retail accounts (78%).

Consumers are clearly completing a range of activities online, which will require organizations to hold their personal data, but more importantly, to secure it.

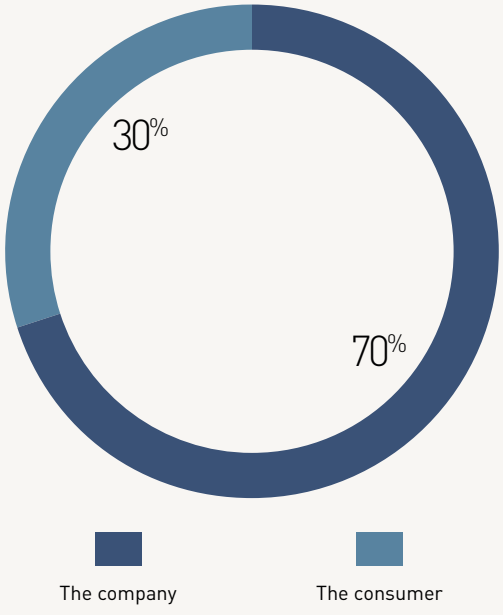
| | |
|---|---|
| 85% | **Online/Mobile banking** |
| 82% | **Social Media accounts** |
| 78% | **Online retail accounts** |

# Company protection and security of customer data

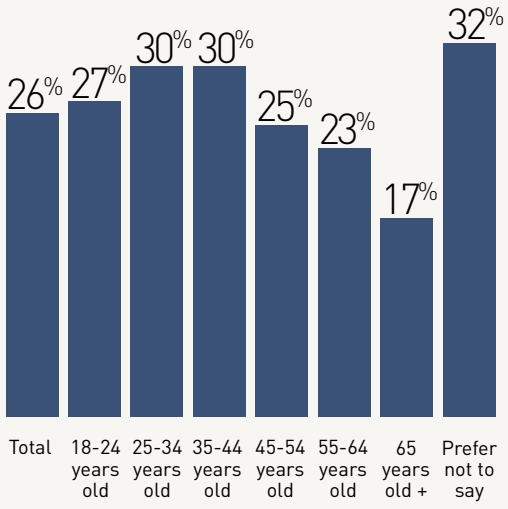
Consumer respondents feel that around 70% (70.10%) of the responsibility for protecting and securing customer data falls on to the company, rather than the customer, on average.

However, it is only just over a quarter (26%) who report that companies take the protection and security of customer data very seriously. Respondents who are 55-64 years old (23%) or 65 years old or above (17%) are the least likely to state that this is the case.

This suggests that the expectation consumers have in companies protecting their data isn't taken as seriously as they would like.




**Analysis of the average percentage of responsibility for protecting and securing customer data that respondents feel falls on to the company and the customer**




**Analysis of respondents who feel that companies take the protection and security of customer data very seriously.**

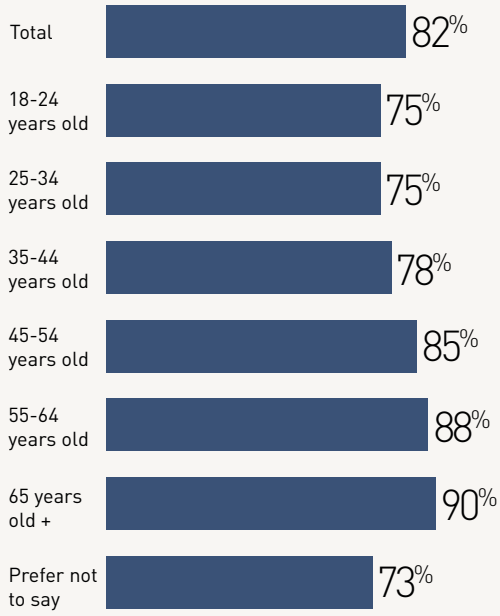
# Security online and providing feedback

Over four in five (82%) respondents agree that they would like organizations to have greater security online.

Respondents aged 65 years old and above (90%) or 55-64 years old (88%) are most likely to agree with this, which may be because they are the age groups to most likely feel that organizations don't take the protection and security of customer data very seriously.

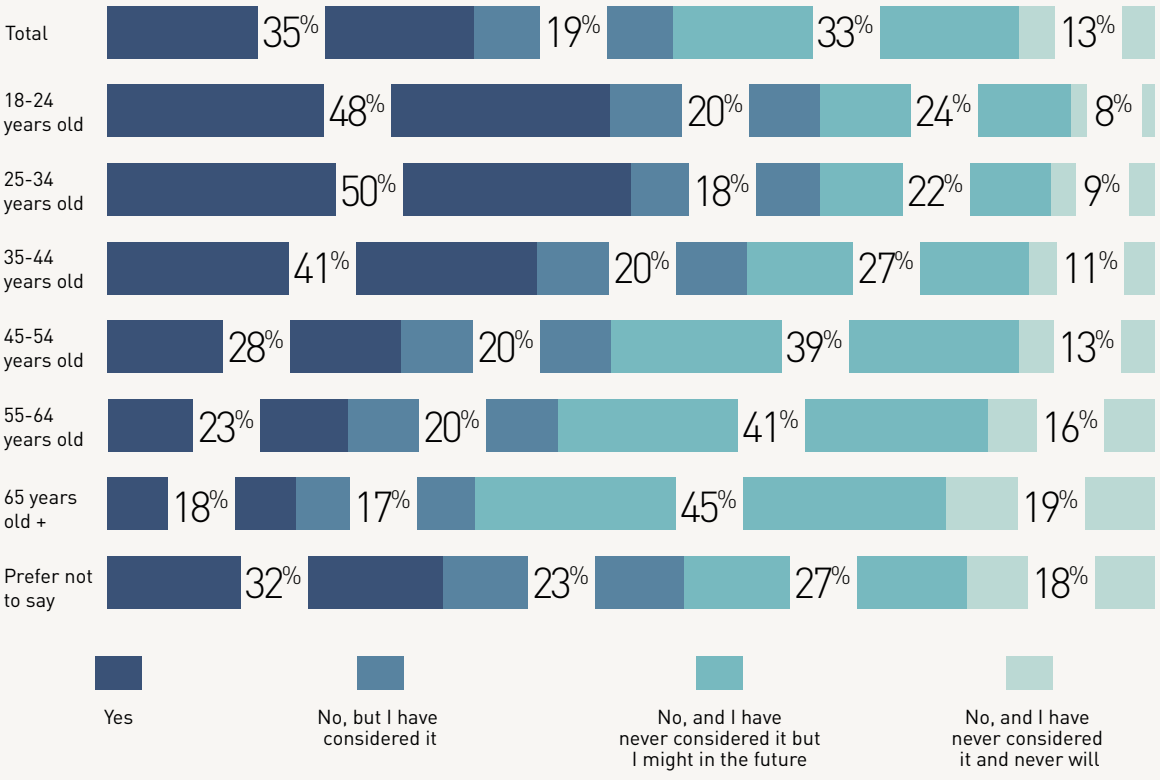
87% of respondents have either already provided organizations with feedback on what security methods they are offering (35%), have considered it (19%) or might in the future (33%).

Respondents of an older age are the most likely to say that they will provide feedback in the future (over 65 years old: 45%, 55-64 years old: 41%), which suggests that they will soon take action upon their concerns.




**Analysis of respondents who would like organizations to have greater security online**

**Analysis of respondents who have or have not ever provided organizations with feedback on what security methods they are offering/using.**

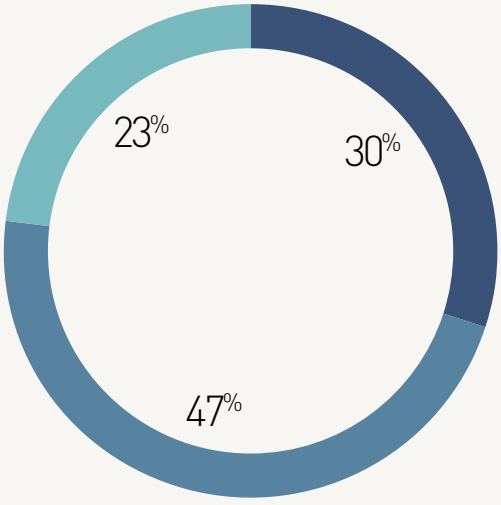


# Two-factor authentication

Of respondents who use online retail accounts, only three in ten (30%) say that they all require two-factor authentication to secure online transactions.

A similar proportion (28%) who use social media sites report that all social media accounts use two-factor authentication.

While many online retailers and social media accounts will use two-factor authentication, there are clearly many that don't or that consumers don't know about, which is likely to explain why only the minority of consumers feel that organizations take the security of customer data very seriously.

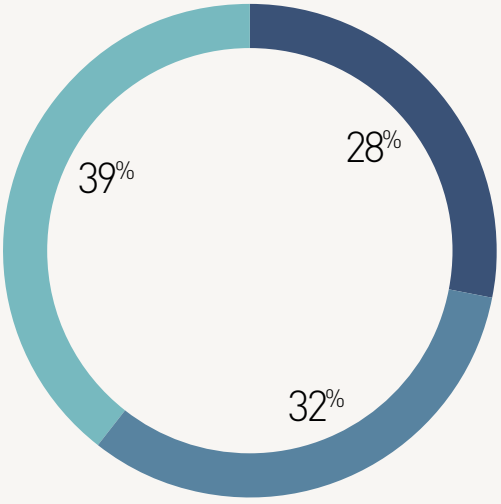



Yes, all of the online retail apps/websites I use do

Yes, some of the online retail apps/websites I use do

No, non of the online retail apps/websites I use do

**Do the online retail apps/websites you use (e.g. Amazon, Ebooker, Expedia etc.) require two-factor authentication to secure online transactions?**




Yes, for all of my social media accounts

Yes, for some of my social media accounts

No, I don't for any of my social media accounts

**Do you use two-factor authentication to secure your Facebook, Twitter, LinkedIn or other social media accounts?**

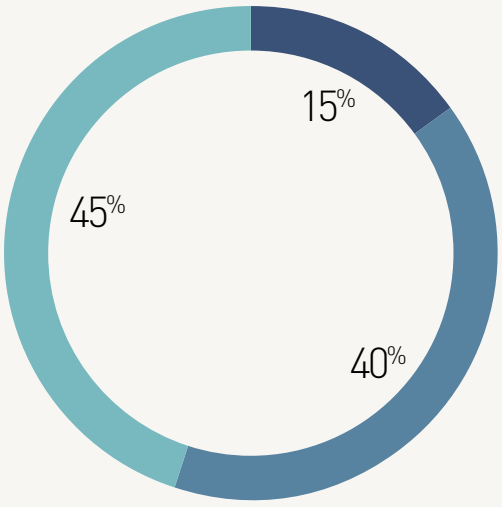
# Using the same password across accounts

Over half (55%) of respondents use the same password across their accounts, with 15% using the same password across all of their accounts, and 40% doing so for some of their accounts.

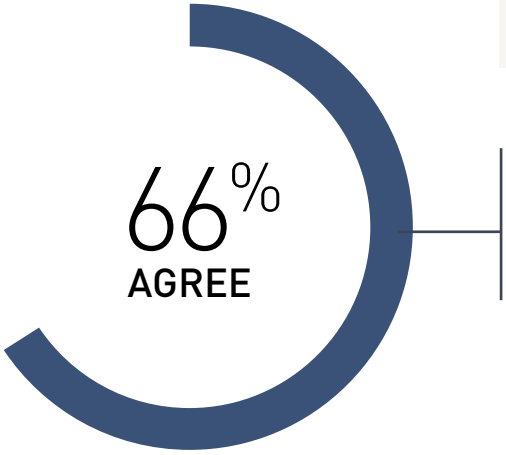
Consumers are leaving themselves vulnerable to attacks by using the same passwords for multiple accounts, which further implies that consumers are relying on the companies to do more to secure their data than they might do themselves.

Two thirds (66%) of those interviewed are worried that at some point their online personal information will be stolen.

This is even more concerning for those that use the same password across accounts as multiple accounts will be at risk of this theft.




**Do you tend to use the same password across all of your accounts? (bank, online retail accounts and social media accounts)**




I am worried that at some point my online personal information will be stolen

# Falling victim to a breach past, present and future

## Falling victim to fraud, theft and breaches

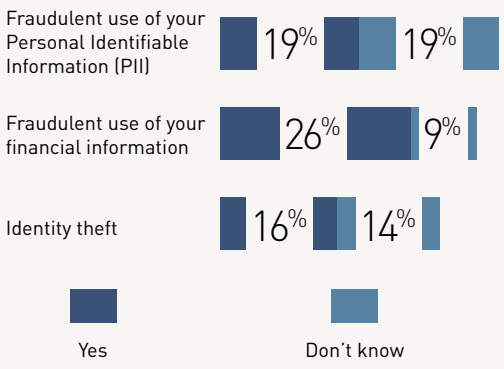
A significant minority of those surveyed have either been a victim of, or are unsure as to whether they've been a victim of, fraudulent use of their Personal Identifiable Information (PII) (38%), fraudulent use of their financial information (35%) and/or identity theft (30%).

What are the most likely causes of being the victim of a breach?

Respondents who have been victim of a breach report the most likely causes as visiting a fraudulent website (43%), clicking a fraudulent web link (42%) and/or phishing (41%).

On average, respondents report three likely causes, which might explain why the majority are concerned about their online personal information being stolen and why some have fallen victim to fraud and theft already.

**Have you been a victim of the following?**



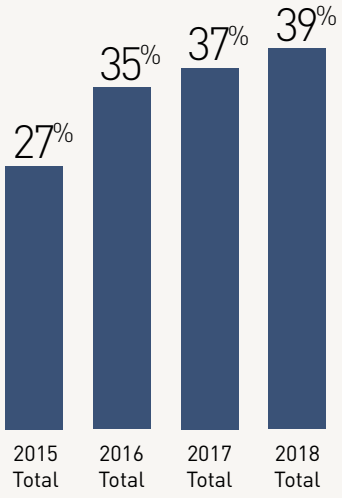

**Which of the following are the most likely causes for you being a victim of a breach?**

# Falling victim to breaches in the future

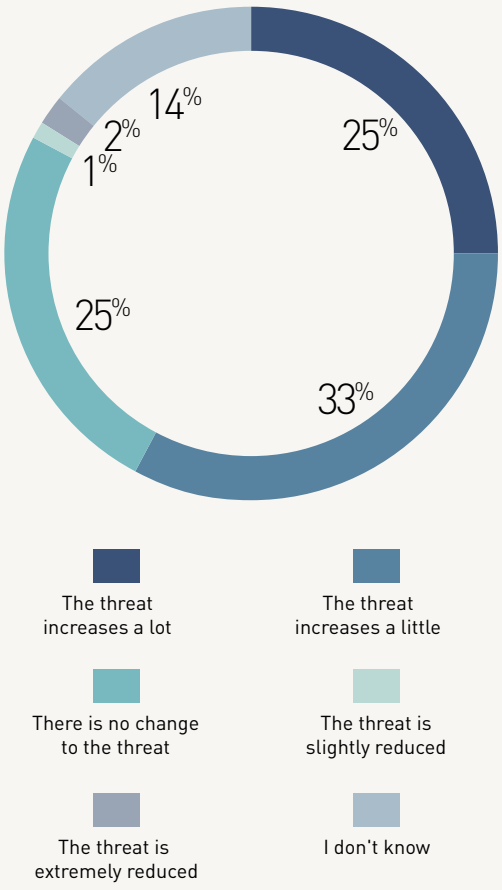
The proportion of surveyed consumers who believe that they are likely to be a victim of a breach at any time has steadily increased over the past four years – 27% in 2015, 35% in 2016, 37% in 2017 and 39% in 2018.

Around six in ten (58%) respondents say that the threat to their personal information increases during a high profile commercial event.

Consumer concerns around breaches are on the rise, suggesting organizations are not improving the way that they secure them from these breaches, especially during peak commercial periods.

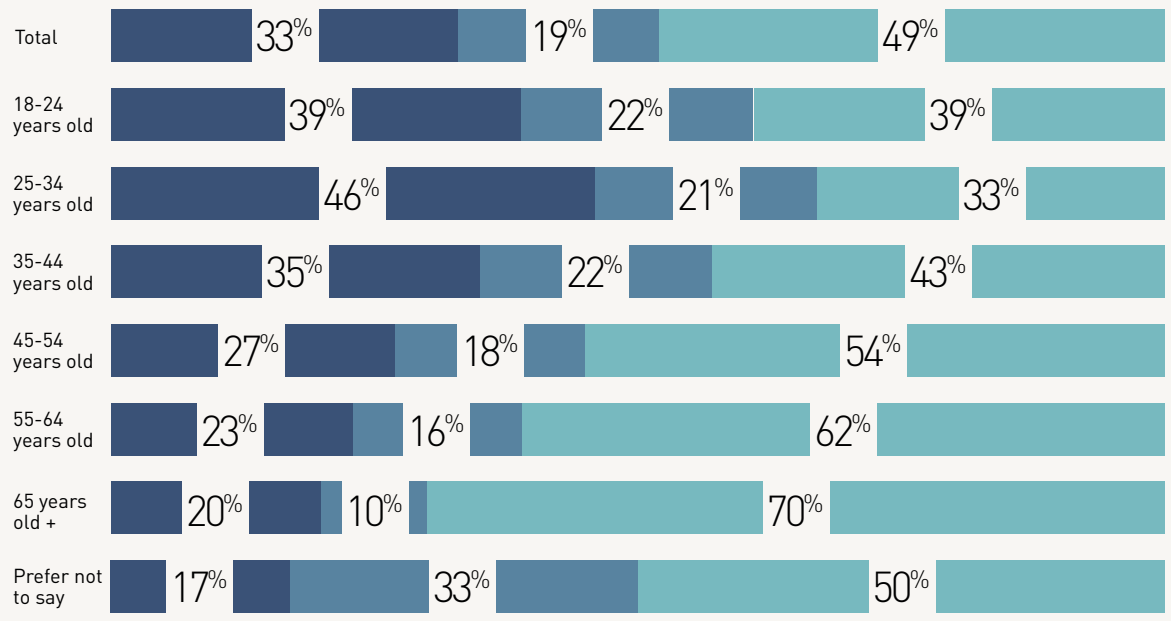



**Analysis of consumers who believe that they are likely to be a victim of a breach at any time**




**How much does the threat to your personal information change during a high profile commercial event (e.g. Black Friday, Amazon Prime Day and Christmas)?**

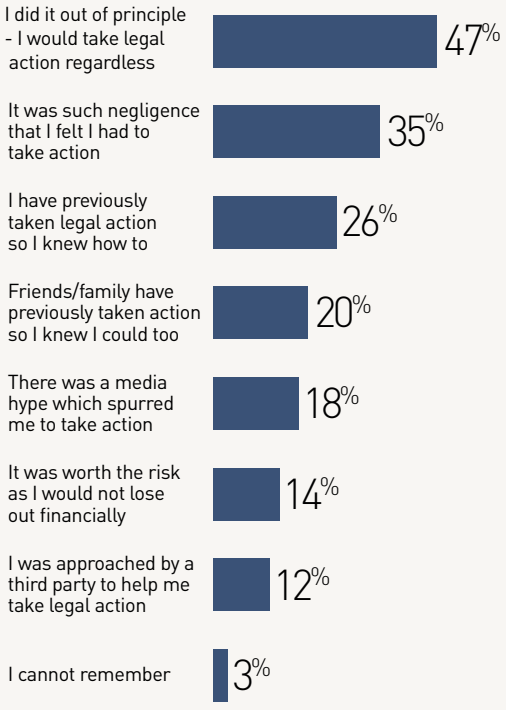
# Legal action following a breach – past and present




A third (33%) of those surveyed have taken legal action against any of the parties involved in exposing/taking their personal information, while around two in ten (19%) are considering doing so.

Approaching half (47%) of those who have already taken legal action did so out of principle and that they would do it regardless of what was exposed, and over a quarter (26%) have previously taken legal action so knew how to.

Customers have many reasons to take legal action if they suffer a breach and some have done so already, which is something organizations should be extremely cautious of, especially with the rising consumer concern around being a victim of a breach.

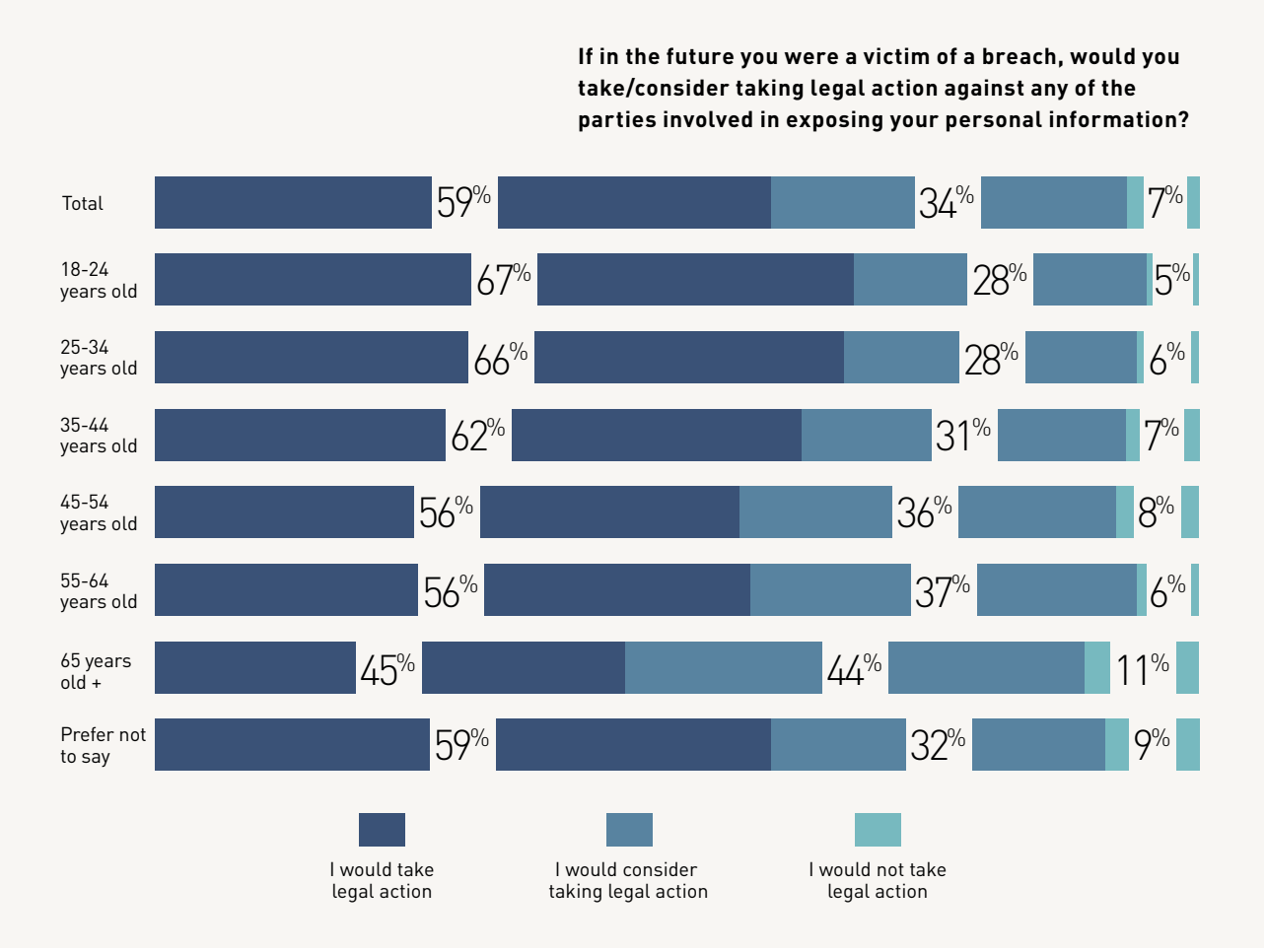


# Legal action following a breach – the future

> Over nine in ten (93%) surveyed consumers would at least consider taking legal action in the future against any parties involved in exposing their personal information.

The proportion of respondents who would take legal action in the future is greater (59%) than those who have already done so (33%).

Organizations are at increasing risk of legal battles if they don't have the correct security in place to protect their customers' data, especially with the likelihood of consumers being victim to a breach expected to rise.



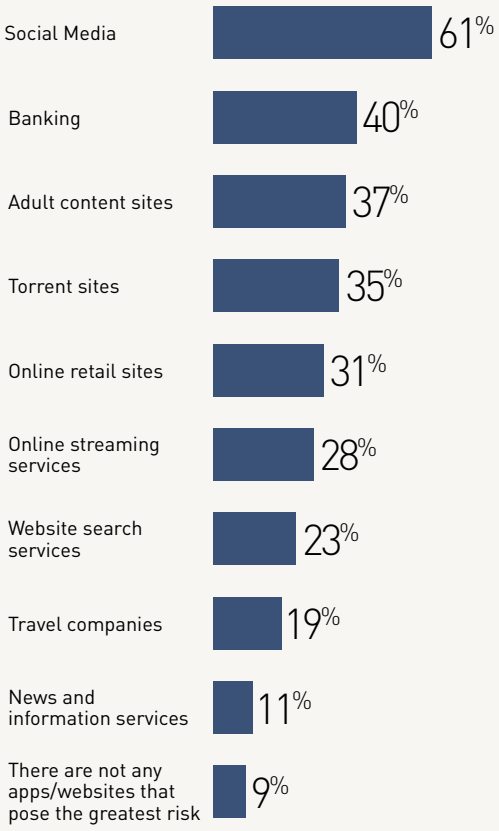
# Where are the risks to consumers?

## Personal information at security risk

Over nine in ten (91%) surveyed consumers believe that there are apps/websites that pose risk in the protection and security of their personal information, which is unsurprising given the majority would like organizations to have greater security online.

The largest proportion (61%) say that social media exposes them to the greatest risk, while over three in ten (31%) say the same for online retail websites.

This may be because of the consumer perception that only the minority use two-factor authentication for these apps/websites but these exposure concerns may also be due to only the minority of consumers feeling that organizations take the security of customer data very seriously.

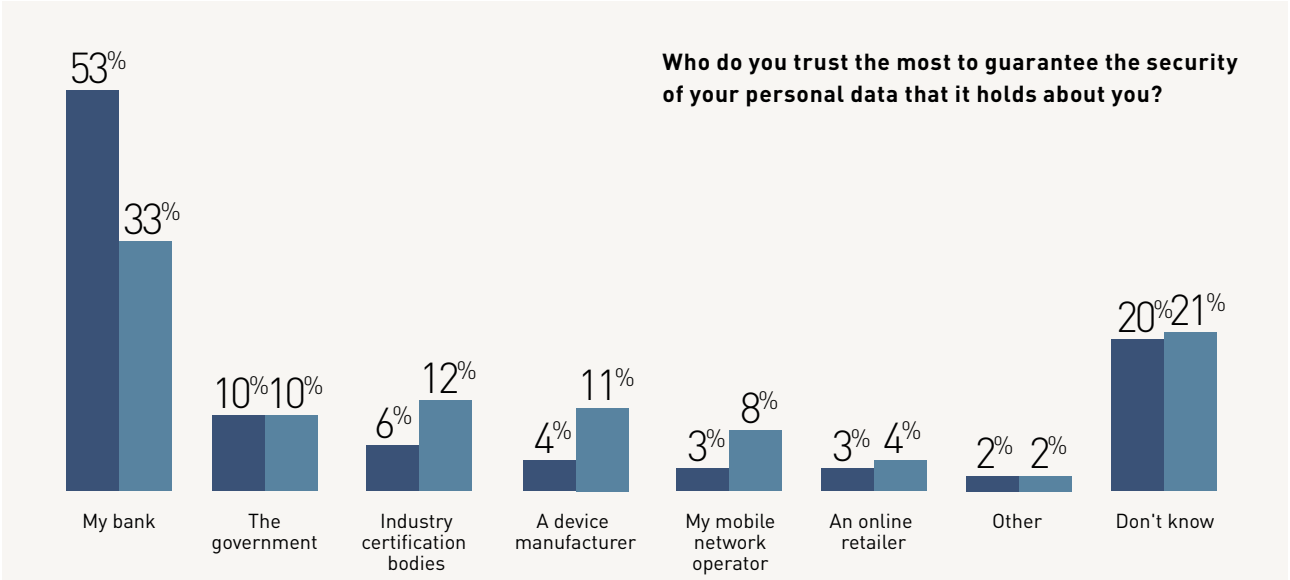



**Which apps/websites do you feel expose you to the greatest risk in the protection and security of your personal information?**

# Who consumers trust the most

Over half (53%) of respondents trust their bank the most to guarantee the security of their personal data that it holds – this is more than the proportion that believe banking exposes them to the greatest risk in the protection and security of their personal information, and has increase from a third (33%) in 2017.

Two in ten (20%) don't know who they trust the most to guarantee the security of their personal data, which could suggest they trust no-one which is possible given the security concerns we have seen.

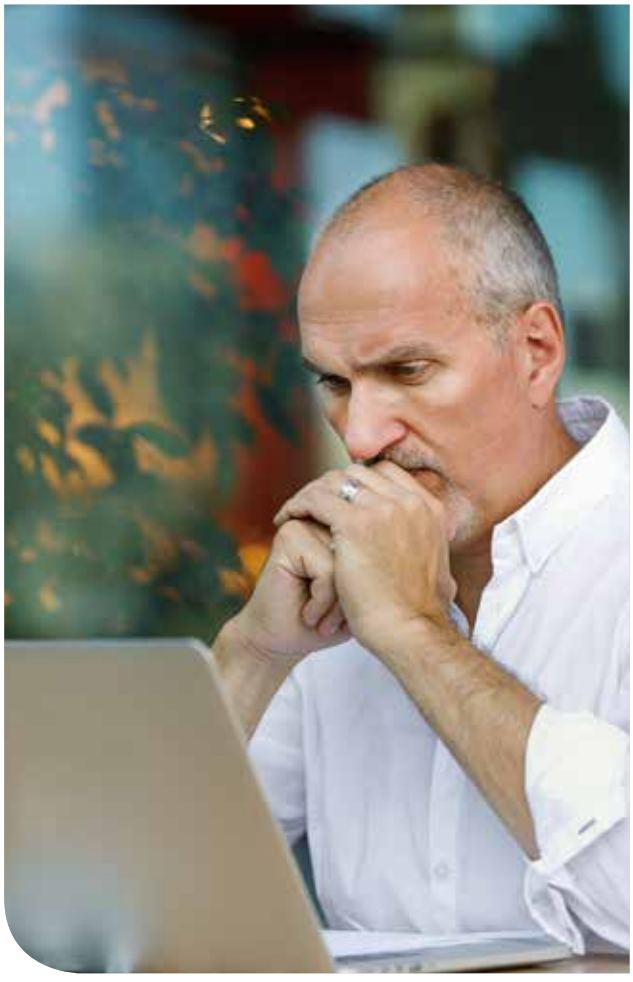



# Direct impact of breaches to businesses

Two thirds (66%) of respondents would be unlikely to shop/do business with an organization that experienced a breach where their financial and sensitive information was stolen. Around half say the same where only their passwords (51%) and/or non-financial information (49%) was stolen, suggesting consumers hold organizations accountable for protecting their personal information and would likely be unforgiving if any aspect was stolen.

This is amplified by the majority of surveyed consumers agreeing that they would stop shopping with a retailer (62%), stop banking with a bank (59%) and/or stop using a social media site (58%) if they suffered an online breach.

It's crucial that organizations have the right security measures in place and build customers' security confidence, otherwise they could lose customers and face legal battles as a result of experiencing a breach.



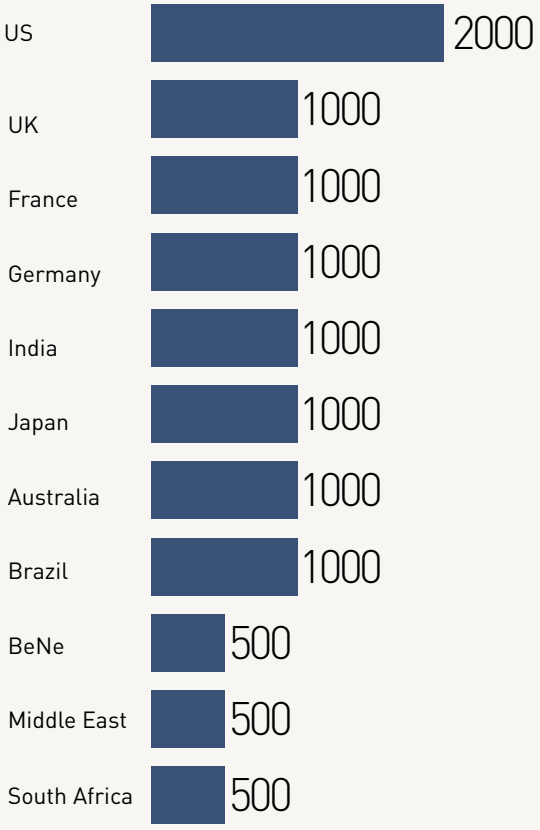
**How likely would you be to shop or do business again with a company (retail, financial, healthcare) that had experienced a breach...**


**Analysis of respondents who agree with the below statements**

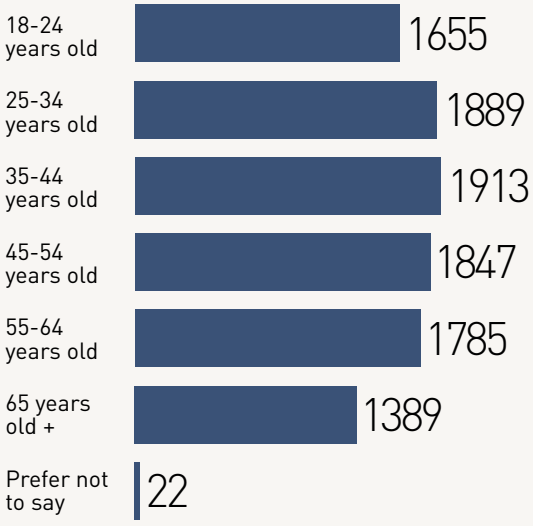
# Demographics

10,500 adult consumers were interviewed in March and April 2018. To qualify, consumers have to actively use online/mobile banking, social media accounts or online retail accounts.

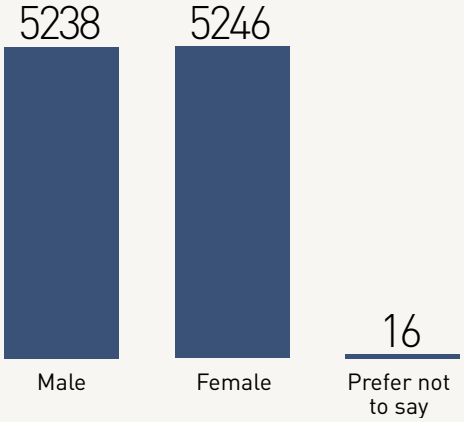
**Respondants split by country**




**Respondants split by age**




**Respondants split by gender**



# A troubled past and frustrated future for consumers

It's unsurprising that consumers are frustrated with the state of data protection within organizations. A quarter of those surveyed have already been a victim of fraudulent use of their financial information (26%), 19% through fraudulent use of their PII, and 16% of identity (ID) theft. Worse, consumers have no faith that things are going to improve, as two-thirds (66%) are worried that at some point in the future their personal information will be stolen.

Even with the fear that they may become victims of a data breach, consumers aren't planning to change their behaviour online as they believe responsibility lies with the companies holding their data. This could explain why over half (55%) of respondents continue to use the same password across different accounts.

In addition to switching brands, young people are more prepared to go further and participate in legal action against brands that lose their data than older generations. Nearly seven in 10 (67%) 18-24-year olds revealed they would take brands that suffered a breach to court, compared to just 45% for 65s and over, with a further 28% of generation z (18-24 year olds) at least considering it.

This should be a wake-up call to businesses that consumer patience has run out. It's clear they have little faith that organizations are taking their data protection seriously, or that their concerns will be heard, forcing them to take action themselves. As young people become the big spenders of the future, businesses are risking not only alienating their current and future revenue streams but also their reputation if they continue to give the impression that they don't take data security seriously. Moving forward businesses must start doing the basics properly; protecting their most valuable asset, data, with the correct security controls.

## ABOUT GEMALTO ENTERPRISE SECURITY

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments, and data – from the edge to the core. Gemalto's portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

**Contact Us:** For more Gemalto research, visit safenet.gemalto.com/data-security-trends/
**Follow Us:** blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free